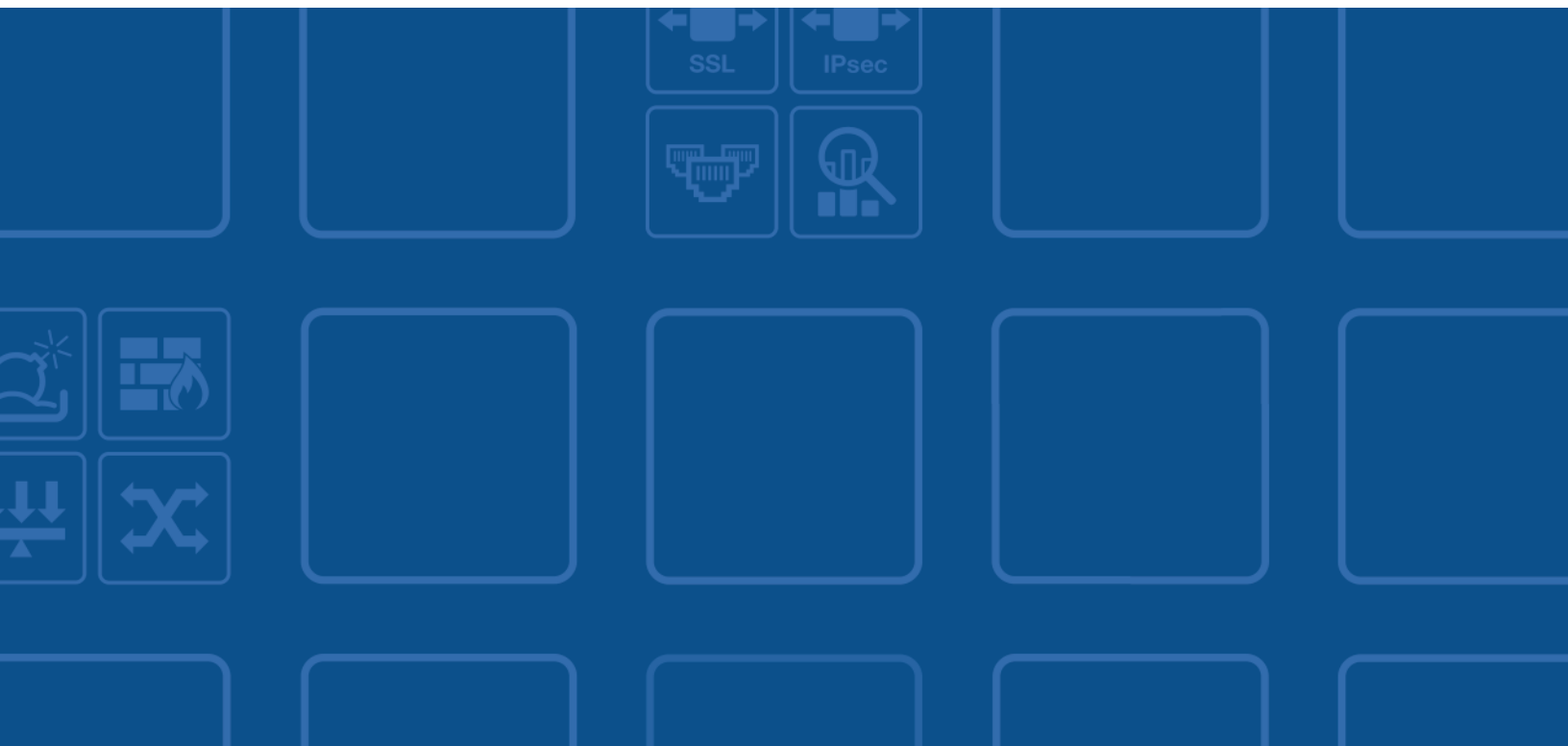
FORTINET
High Performance Network Security

FortiClient EMS for Chromebooks - QuickStart Guide

VERSION 1.2.0



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

June 15, 2017

FortiClient EMS for Chromebooks 1.2.0 QuickStart Guide

04-120-408700-20170615

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-06-15	Initial release

Introduction

This guide describes how to install and set up FortiClient Enterprise Management Server (EMS) for Chromebooks. It also describes how to set up Google Admin console to use the FortiClient Web Filter extension. Together the products provide web filtering for Google Chromebook users.

Supported installation platforms

You can install FortiClient EMS for Chromebooks on the following platforms:

- Microsoft Windows Server 2012, 2012 R2
- Microsoft Windows Server 2008 R2

For information about minimum system requirements and the latest information about supported platforms, see the *FortiClient EMS for Chromebooks Release Notes*, available in the Fortinet Document Library.

Requirements

The following components and knowledge are required to use FortiClient EMS for Chromebooks:

- FortiClient EMS for Chromebooks installer
- FortiClient Web Filter extension available in the Google Web Store for Chrome OS
- Google For Work account
- Knowledge of administering the Google Admin console
- A domain configured in Google Admin console
- SSL certificate to support communication between FortiClient Web Filter extension and FortiClient EMS for Chromebooks
- SSL certificate to support communication between FortiClient Web Filter extension and FortiAnalyzer for logging, if using
- Unique set of Service Account Credentials

Required services and ports

You must ensure that required ports and services are enabled for use by FortiClient EMS for Chromebooks and its associated applications on your server. The required ports and services enable FortiClient EMS for Chromebooks to communicate with endpoints and servers running associated applications.

Communication	Service	Protocol	Port
Apache	HTTPS	TCP	443
SQL server			
FortiClient on Chrome OS • Connection to Profile Server.			8443 (default) You can customize this port.

Google for Work account

You will need to sign up for your own *Google For Work* account before you can use the Google service and manage your Chromebook users.

The *Google for Work* account is different from the free consumer account. The *Google for Work* account is a paid account that gives you access to a range of Google tools, services and technology.

You can sign up for a Google for Work account here: https://www.google.com/a/signup/#0

In the sign up process, you will need to use your email address to verify your Google Domain. This is also to prove that you have ownership of the domain.

SSL certificates

FortiClient EMS for Chromebooks requires an SSL certificate signed by a Certificate Authority (CA) in pfx format. Use your CA to generate a certificate file in pfx format, and remember the configured password. For example, the certificate filename is *server.pfx* with password 111111.

The server where FortiClient EMS for Chromebooks is installed should have an FQDN (fully qualified domain name), such as ems.forticlient.com, and you must specify the FQDN in your SSL certificate.

If you're using a public SSL certificate, the FQDN can be included in either *Common Name* or *Subject Alternative Name*. You must add the SSL certificate to FortiClient EMS for Chromebooks. See Adding SSL certificates to FortiClient EMS for Chromebooks on page 26. You do not need to add the root certificate to Google Admin console.

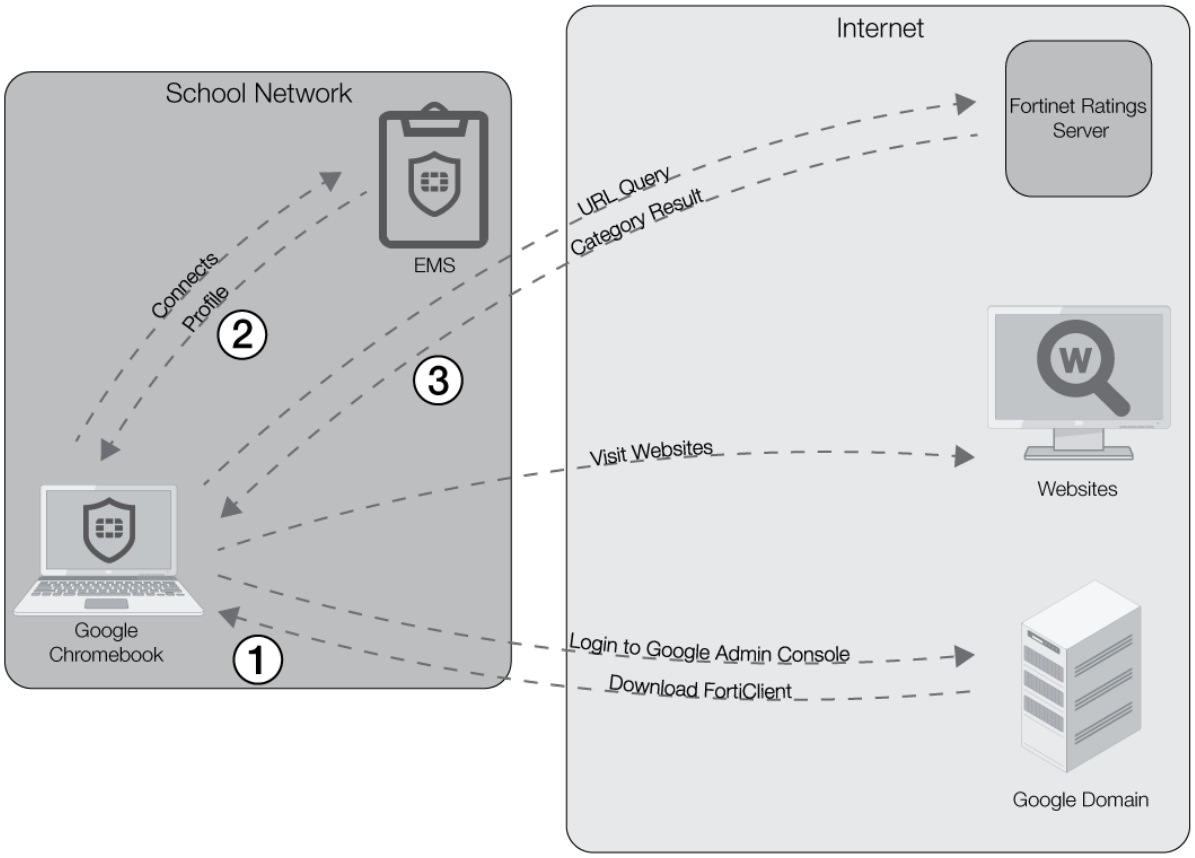
If you're using a self-signed certificate (non-public SSL certificate), the *Subject Alternative Name* of your certificate must include `DNS:<FQDN>`, for example, `DNS:ems.forticlient.com`. You must add the SSL certificate to FortiClient EMS for Chromebooks, and you must add the root certificate to Google Admin console to allow the extension to trust FortiClient EMS for Chromebooks. See Adding root certificates on page 14.

How the products work together

After you install and configure FortiClient EMS for Chromebooks, Google Admin Console, and the FortiClient Web Filter extension, the products work together to provide web-filtering security for Google Chromebook users

that are logged into the Google domain. Following is a summary of how the products work together after the setup is complete:

1. When Google Chromebook users log into Google Chromebook, Google Chromebook downloads the FortiClient Web Filter extension.
2. FortiClient connects to FortiClient EMS for Chromebooks, and downloads a profile to Google Chromebook. The profile contains the web-filtering settings from FortiClient EMS for Chromebooks.
3. When Google Chromebook users browse the Internet, FortiClient sends the URL query to the Fortinet Ratings Server, and the Fortinet Ratings server returns the category result to FortiClient. FortiClient compares the category results with the profile to determine whether to allow the Google Chromebook user to access the URL.



Installation

Following is a summary of how to install and start FortiClient EMS for Chromebooks:

1. Download the installation file. See Downloading the installation file on page 9.
2. Install FortiClient EMS for Chromebooks. See Installing FortiClient EMS for Chromebooks on page 9.
3. Start FortiClient EMS for Chromebooks and log in. See Starting FortiClient EMS for Chromebooks and logging in on page 11.

Downloading the installation file

FortiClient EMS for Chromebooks is available for download from the following location:

- Fortinet Support website: https://support.fortinet.com/

You can also receive the installation file from a sales representative.

The following installation file is available for FortiClient EMS for Chromebooks:

- `FortiClientEnterpriseManagement_Chromebook_1.2.0.<build>_x64.exe`

For more information about obtaining FortiClient EMS for Chromebooks, contact your Fortinet reseller.

Installing FortiClient EMS for Chromebooks

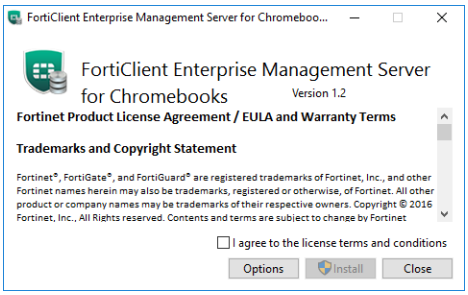
The FortiClient EMS for Chromebooks installation package includes:

- FortiClient EMS for Chromebooks
- Microsoft SQL Server 2014 Express Edition
- Apache HTTP server

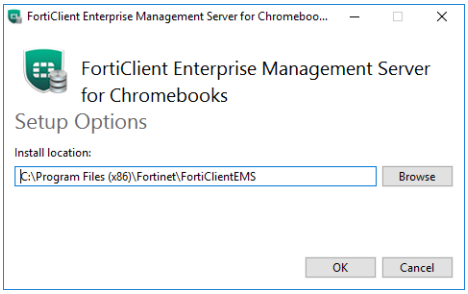
Local administrator rights and Internet access are required to install FortiClient EMS for Chromebooks.

To install FortiClient EMS for Chromebooks:

1. If you are logged into the system as an administrator, double-click the downloaded installation file.
   If you are not logged in as an administrator, right-click on the installation file, and select *Run as administrator* from the pop-up menu.
2. If applicable, select *Yes* in the *User Account Control* window to allow the program to make changes to your system.
3. In the installation window, select *I agree to the license terms and conditions*, if you agree with the license terms and conditions. If you do not agree, you cannot install the software.



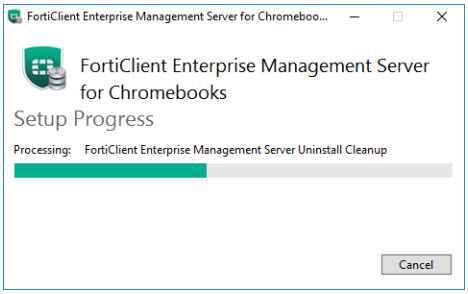
4. (Optional) Click *Options* to specify a custom directory for the FortiClient EMS for Chromebooks installation.



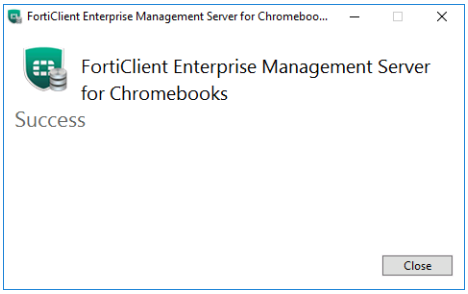
   a. Click *Browse* to locate and select the custom directory.
   b. Click *OK* to return to the installation wizard.

5. Click *Install*.

   The installation may take 30 minutes or longer. It may appear to stop at times, but this is only because certain steps in the installation process take longer than others. Please be patient.



6. When the program has installed correctly, the *Success* window will be displayed. Click *Close* to close the window.



   A *FortiClient Enterprise Management Server* icon will be added to the desktop.

Starting FortiClient EMS for Chromebooks and logging in

FortiClient EMS for Chromebooks runs as a service on Windows computers.

To start FortiClient EMS:

1. Double-click the *FortiClient Enterprise Management Server for Chromebooks* icon to start FortiClient EMS.
2. Sign in with username *admin* and no password.
3. Change the username and password by going to *View* > *User Management* > *Administration*.
4. Configure FortiClient EMS for Chromebooks by going to *View* > *Settings*.

Accessing FortiClient EMS remotely

You can access FortiClient EMS for Chromebooks remotely by using a web browser instead of the GUI.

To enable remote access to FortiClient EMS for Chromebooks:

1. Go to *View* > *Settings*.
2. On the *Server Settings* tab, enable *Remote Administration HTTPS Access*.
3. In the *Custom Host Name* box, type the host name or IP address.
4. Click *Save*.

To remotely access FortiClient EMS for Chromebooks:

- To access EMS from the EMS server, visit `https://localhost`
- To access the server remotely, use the server's hostname: `https://<server_name>`
  Ensure that you can ping `<server_name>` remotely. This can be achieved by adding it into a DNS entry or by adding it to the Windows hosts file. You may have to modify the Windows firewall rules to allow the connection.

Google Admin Console Setup

This section describes how to add and configure the FortiClient Web Filter extension on Chromebooks that are enrolled in the Google domain.

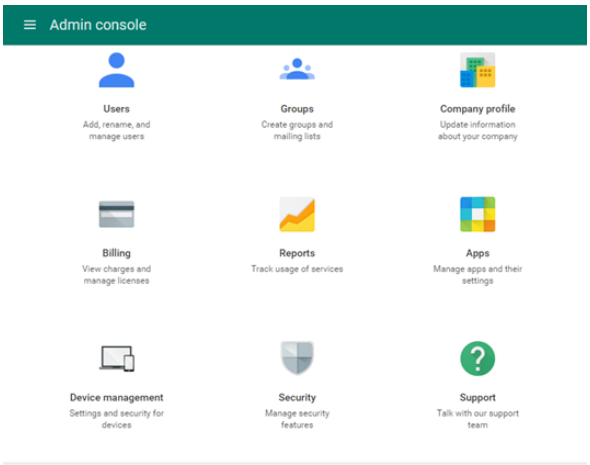
Following is a summary of how to set up Google Admin console:

1. Log into Google Admin console. See Logging into Google Admin console on page 12
2. Add the FortiClient Web Filter extension. See Configuring the FortiClient Web Filter extension on page 13.
3. Configure the FortiClient Web Filter extension. See Configuring the FortiClient Web Filter extension on page 13.
4. Add the root certificate. See Adding root certificates on page 14.

Logging into Google Admin console

To log in to Google Admin console:

1. Log in to Google Admin console (https://admin.google.com) by using your Google Domain admin account. The Admin console is displayed.



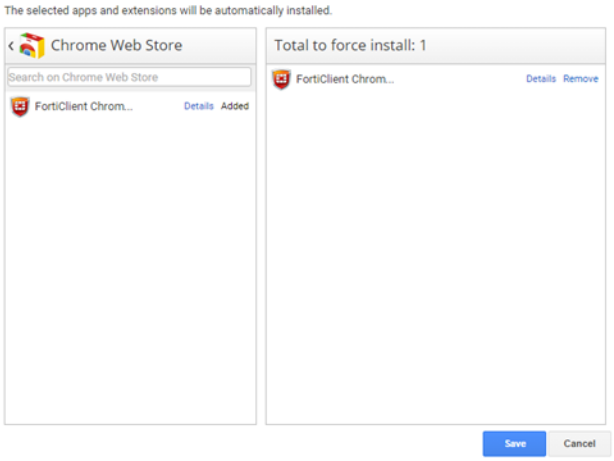
Adding the FortiClient Web Filter extension

FortiClient EMS for Chromebooks software is not available for public use. You can only enable the feature by using the following extension ID: igbg-pehnbmhgdgjbhkkpedommgmfbeao

To add the FortiClient Web Filter extension:

1. In Google Admin console, go to *Device management* > *Chrome Management* > *User Settings* > *Apps and Extensions* > *Force-installed Apps and Extensions* > *Manage force-installed apps*.

2. Select *Chrome Web Store*, and search for the following extension ID: igbgpehnbmhgdgjbhkkpedommgmfbeao.
3. Add the extension ID and save.
   The extension name is displayed as *FortiClient Chromebook Web Filter Extension*.



Configuring the FortiClient Web Filter extension

You must configure the FortiClient Chromebook Web Filter extension to enable Google Admin console to communicate with FortiClient EMS for Chromebooks.

FortiClient EMS for Chromebooks hosts the services that assign endpoint profiles of web-filtering policies to groups in the Google domain. FortiClient EMS for Chromebooks also handles the logs and web-access statistics sent from the FortiClient Web Filter extensions.

FortiClient EMS for Chromebooks is the profile server.

To configure the FortiClient Web Filter extension:

1. In FortiClient EMS for Chromebooks, locate the server name and port by going to *View* > *Settings*.
2. Create a text file that contains the following text:

```
{
   "ProfileServerUrl": { "Value": "https://< ProfileServer >:< port for Profile Server >"}
}
```

   For example:

```
{
   "ProfileServerUrl": { "Value": "https://ems.mydomain.com:8443”}
}
```

3. In Google Admin console, go to *Device management* > *Chrome Management* > *App Management* > *FortiClient Chrome Web Filter Extension* > *User settings*.
4. Click a domain or organization unit (OU).
5. In the right pane, under *Configure*, upload a new configuration file.
   You can also view the current settings.

6. Click *Save*.
7. Go to *Device Management* > *Chrome* > *App Management*, to view your Configured Chrome Apps.

Adding root certificates

This section includes the following information:

Communication with FortiClient Chromebook Web Filter extension

The FortiClient Chromebook Web Filter extension communicates with FortiClient EMS for Chromebooks by using HTTPS connections. The HTTPS connections require an SSL certificate. You must obtain an SSL certificate and add the certificate to FortiClient EMS for Chromebooks to allow the extension to trust FortiClient EMS for Chromebooks.

If you use a public SSL certificate, you only need to add the public SSL certificate to FortiClient EMS for Chromebooks. See Adding SSL certificates to FortiClient EMS for Chromebooks on page 26.

However, if you prefer to use a certificate that is not from a common CA, you must add the SSL certificate to FortiClient EMS for Chromebooks, and you must also push the root CA of your certificate to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiClient EMS for Chromebooks will not work. See Uploading root certificates to Google Admin console on page 15.

Communication with FortiAnalyzer for logging

This section applies only if you are sending logs from FortiClient EMS for Chromebooks to FortiAnalyzer. If you are not sending logs, you can skip this FortiAnalyzer section.

Sending logs to FortiAnalyzer requires that you enable ADOMs in FortiAnalyzer and add FortiClient EMS for Chromebooks to FortiAnalyzer. FortiClient EMS for Chromebooks is added as a device to the FortiClient ADOM in FortiAnalyzer. For information on enabling ADOMs and adding a device to FortiAnalyzer, see the *FortiAnalyzer Administration Guide*.

FortiClient EMS for Chromebooks supports logging to FortiAnalyzer. If you have a FortiAnalyzer device and configure FortiClient EMS for Chromebooks to send logs to FortiAnalyzer, a FortiAnalyzer CLI command must be enabled and an SSL certificate is required to support communication between FortiClient Web Filter extension and FortiAnalyzer.

If you use a public SSL certificate, you only need to add the public SSL certificate to FortiAnalyzer. See Adding SSL certificates to FortiAnalyzer on page 28.

However, if you prefer to use a certificate that is not from a common CA, you must add the SSL certificate to FortiAnalyzer, and you must also push the root CA of your certificate to the Google Chromebooks. Otherwise, the

HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiAnalyzer will not work. See Uploading root certificates to Google Admin console on page 15.

The FortiAnalyzer IP address should be specified in the SSL certificate. If you're using a public SSL certificate, the FortiAnalyzer IP address can be assigned to either *Common Name* or *Alternative Name*. If you're using a self-signed (nonpublic) SSL certificate, the *Subject Alternative Name* of your certificate must include `IP:<FortiAnalyzer IP>`.

Summary of where to add certificates

The following table summarizes where to add certificates to support communication with FortiClient Web Filter extension and with FortiAnalyzer.

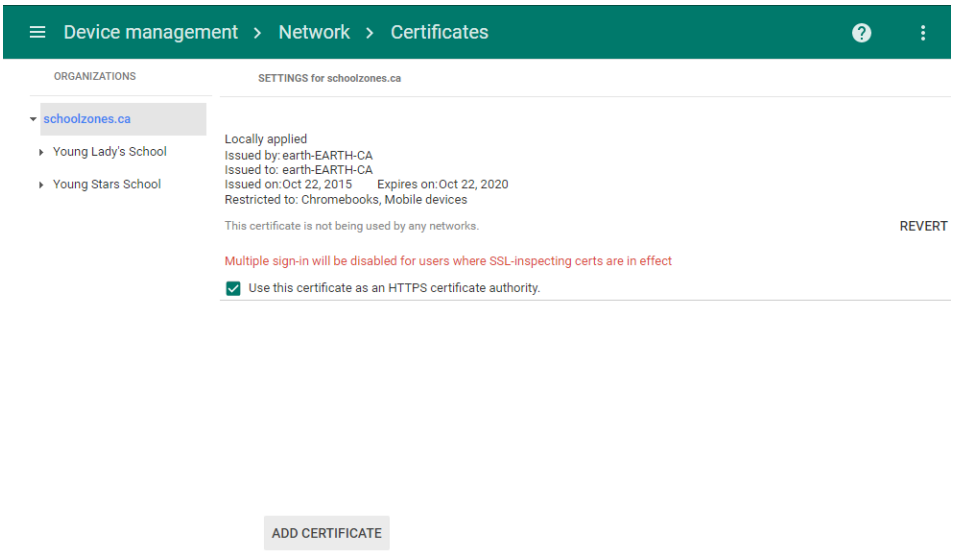
Scenario	Certificate and CA	Where to Add Certificates
Allow FortiClient Chromebook Web Filter extension to trust EMS	Public SSL certificate	• Add SSL certificate to FortiClient EMS for Chromebooks.
	SSL certificate not from a common CA	• Add SSL certificate to FortiClient EMS for Chromebooks. • Add the root CA of your certificate to Google Admin console.
Allow FortiClient Chromebook Web Filter extension to trust FortiAnalyzer for logging	Public SSL certificate	• Add SSL certificate to FortiAnalyzer.
	SSL certificate not from a common CA	• Add SSL certificate to FortiAnalyzer. • Add the root CA of your certificate to Google Admin console.

Uploading root certificates to Google Admin console

To add root certificates:

1. In Google Admin console, go to *Device Management* > *Network* > *Certificates (root certificate) (crt certificate)*.
2. Add the root certificate.
3. Select the *Use this certificate as an HTTPS certificate authority* check box.

Do not forget to select the *Use this certificate as an HTTPS certificate authority* check box.



Disabling access to Chrome developer tools

It is recommended to disable access to Chrome developer tools. This blocks students from disabling the FortiClient Web Filter extension.

To disable access to Chrome developer tools:

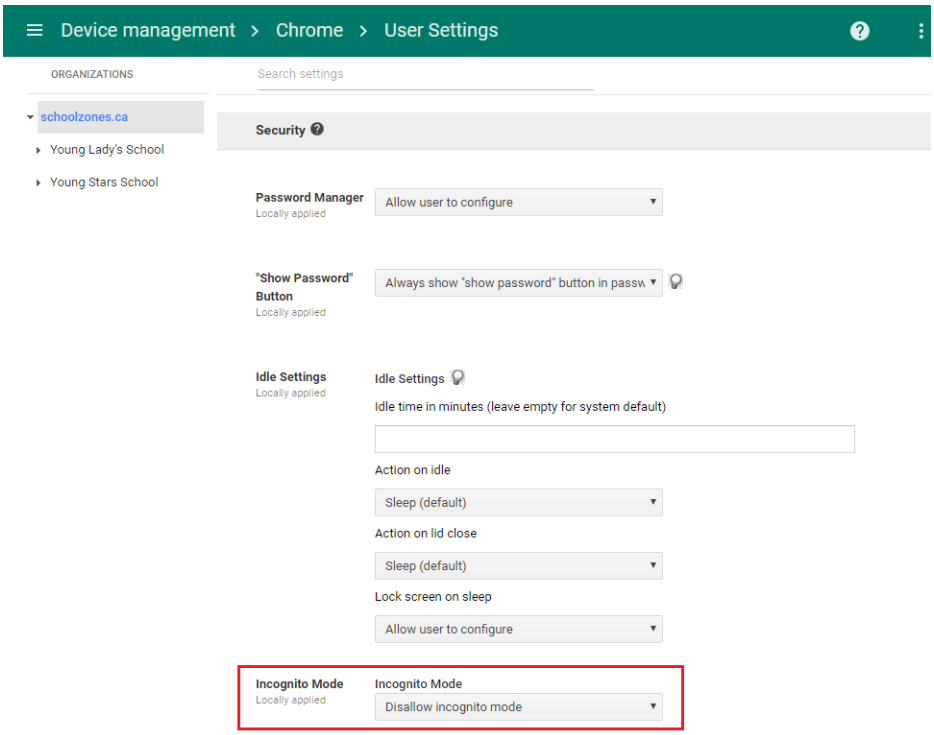
1. In Google Admin console, go to *Device management* > *Chrome Management* > *User Settings*.
2. For the *Developer Tools* option, select *Never allow user of built-in developer tools*.

Disallowing incognito mode

When users browse in incognito mode, extensions will be bypassed. Incognito mode should be disallowed for managed Google domains.

To disallow incognito mode:

1. In Google Admin console, go to *Device management* > *Chrome management* > *User settings*.
2. From the left panel, select the organization.
3. In the *Security* section, set *Incognito Mode* to *Disallow incognito mode*.



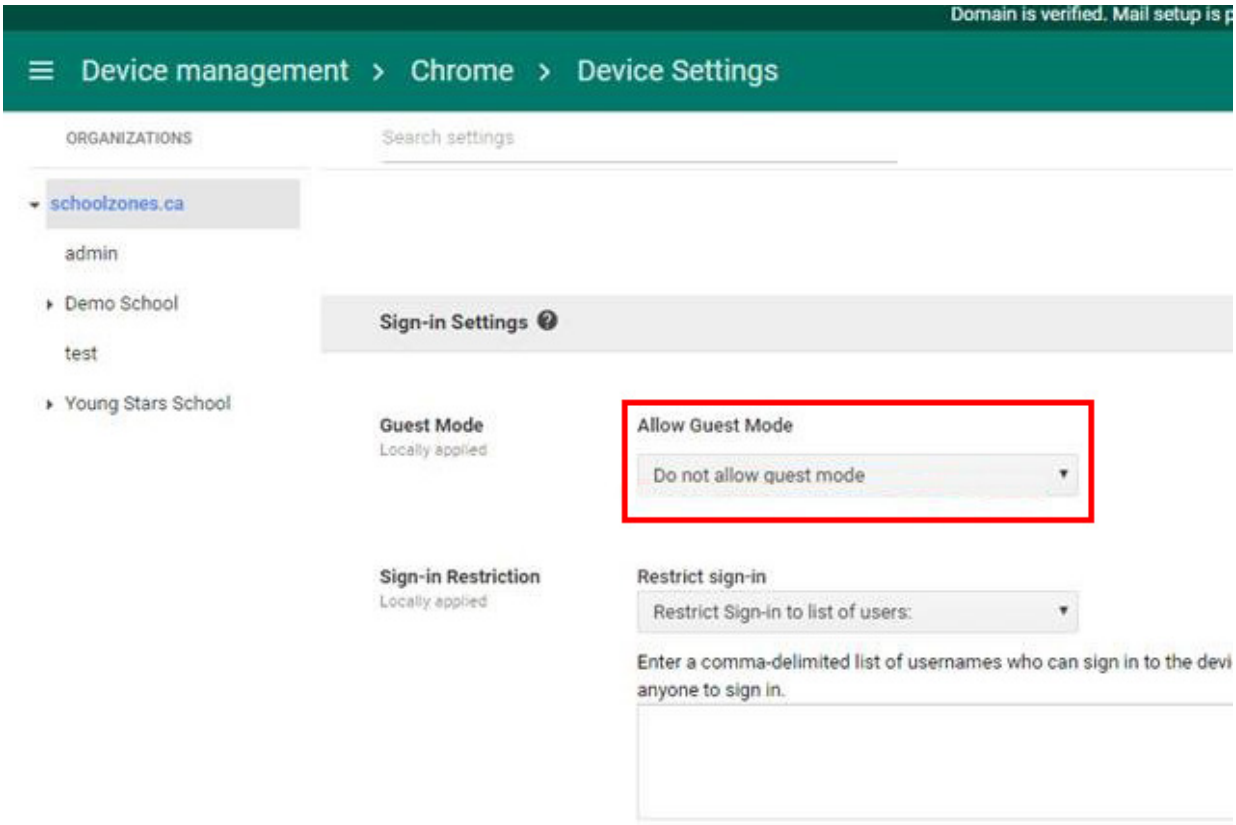
4. Click *Save*.

Disallowing guest mode

Guest mode should be disallowed for managed Google domains.

To disallow guest mode:

1. In Google Admin console, go to *Device management* > *Chrome management* > *Device settings* > *Sign-in settings*.
2. From the left panel, select the organization.
3. Under *Guest Mode* > *Allow Guest Mode* > select *Do not allow guest mode* from the drop down.



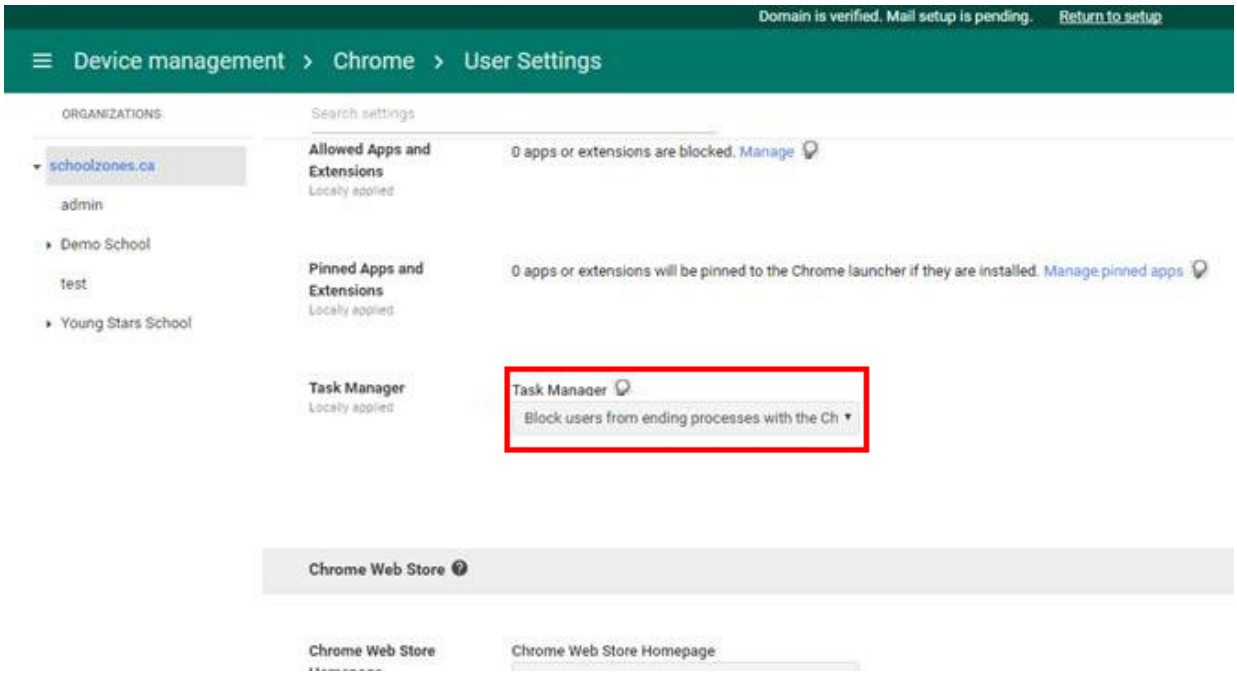
4. Click *Save*.

Blocking Task Manager

Task Manager should be blocked for managed Google domains.

To block Task Manager:

1. In Google Admin console, go to *Device Management* > *Chrome Management* > *User settings* > *Apps and Extensions*.
2. From the left panel, select the organization.
3. Under *Task Manager* select *Block users from ending processes with the Chrome Task Manager* from the drop down.


Domain is verified. Mail setup is pending. Return to setup
Device management > Chrome > User Settings
ORGANIZATIONS
schoolzones.ca
admin
Demo School
test
Young Stars School
Search settings
Allowed Apps and Extensions
Locally applied
0 apps or extensions are blocked. Manage
Pinned Apps and Extensions
Locally applied
0 apps or extensions will be pinned to the Chrome launcher if they are installed. Manage pinned apps
Task Manager
Locally applied
Task Manager
Block users from ending processes with the Ch
Chrome Web Store
Chrome Web Store
Chrome Web Store Homepage

4. Click *Save*.

Service Account Credentials

FortiClient EMS for Chromebooks requires Service Account Credentials generated by the Google Developer console. You can use the default Service Account Credentials provided with FortiClient EMS for Chromebooks, or you can generate and use unique Service Account Credentials, which is more secure.

This section describes how to configure default and unique Service Account Credentials. See the following sections:

- Configuring default Service Account Credentials on page 20
- Configuring unique Service Account Credentials on page 21

The Service Account Credentials must be the same in FortiClient EMS for Chromebooks and Google Admin console.

Configuring default Service Account Credentials

FortiClient EMS for Chromebooks includes the following default Service Account Credentials generated by the Google Developer console:

Option	Default Setting	Where Used
Client ID	102515977741391213738	Google Admin console
Email address	account-1@forticli-entwebfilter.iam.gserviceaccount.com	FortiClient EMS for Chromebooks
Service Account Certificate	A certificate in `.pem` format for the Service Account Credentials	FortiClient EMS for Chromebooks

The Service Account Credentials are a set. If you change one of the credentials, you must also change the other two credentials.

Adding the default Service Account Client ID to Google Admin Console

To configure the default Service Account Credentials, you must add the default value for the Client ID to Google Admin Console. No other configuration for Service Account Credentials is required. See Adding Service Account Credentials to Google Admin Console on page 24.

Configuring unique Service Account Credentials

When using unique Service Account Credentials for improved security, you must complete the following steps to add the unique Service Account Credentials to Google Admin console and FortiClient EMS for Chromebooks:

1. Create unique Service Account Credentials by using Google Developer console. See Creating unique Service Account Credentials on page 21.
2. Add the unique Service Account Credentials to Google Admin console. See Adding Service Account Credentials to Google Admin Console on page 24.
3. Add the unique Service Account Credentials to FortiClient EMS for Chromebooks. See Adding Service Account Credentials to EMS on page 25.

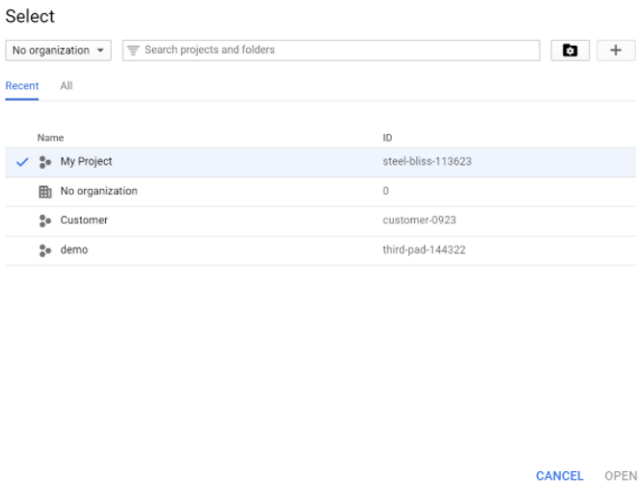
Creating unique Service Account Credentials

Creating a unique set of Service Account Credentials provides more security. Unique Service Account Credentials include the following:

- Client ID (a long number)
- Service Account ID (Email address)
- Service Account Certificate (a certificate in `.pem` format)

To create a unique service account:

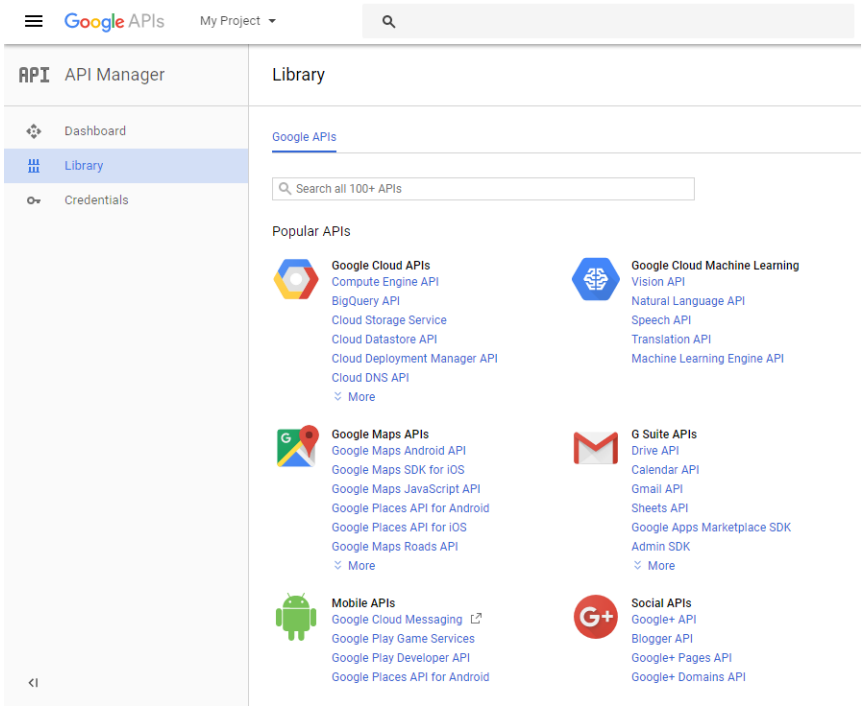
1. Go to https://console.developers.google.com.
2. Log in with your Google for Work account credentials.
3. Create a new project.
   a. Click the toolbar list. The browser displays the following dialog.



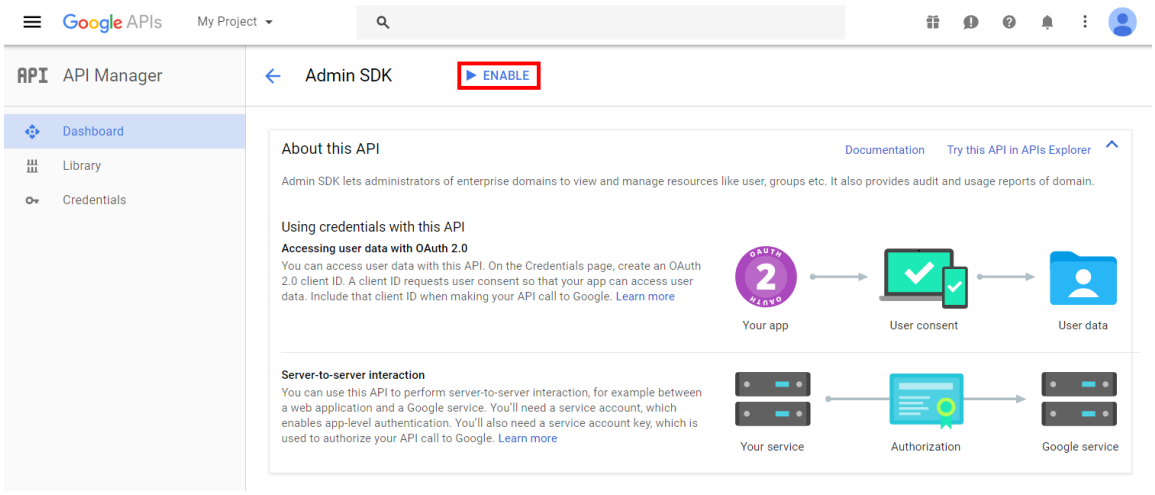
   b. Select your organization, if you see an organization dropdown list.
   c. Click the + button.
   d. In the *Project name* field, enter your project name, then click *Create*.
4. Enable the Admin SDK.

a. Select your project from the toolbar list, then go to the *Library* tab.

b. Under *G Suite APIs*, click *Admin SDK*.



c. Click *ENABLE*.



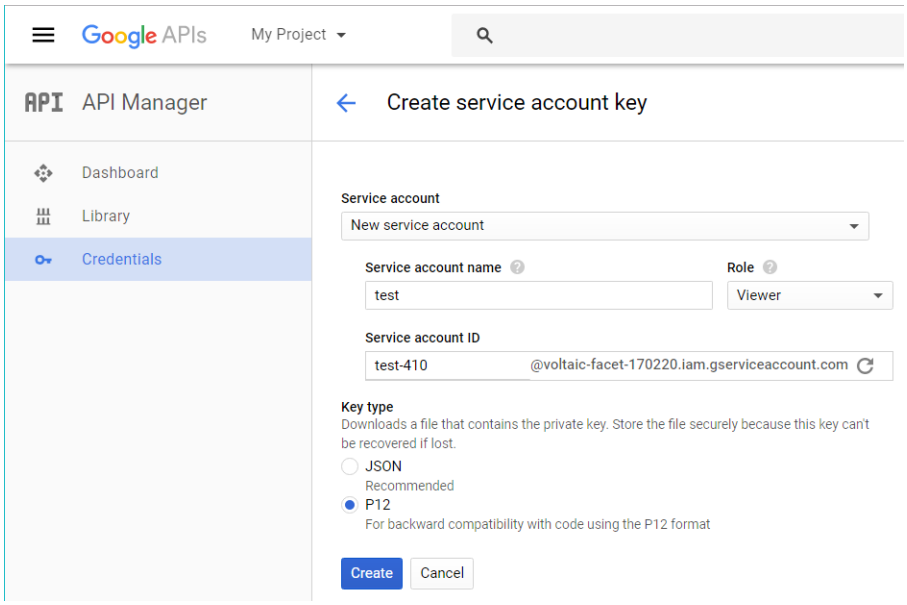
5. Create a service account.

a. Go to the *Credentials* tab and select *Create Credentials* > *Service account key*.

b. From the *Service account* list, select *New Service Account*. Enter a service account name.

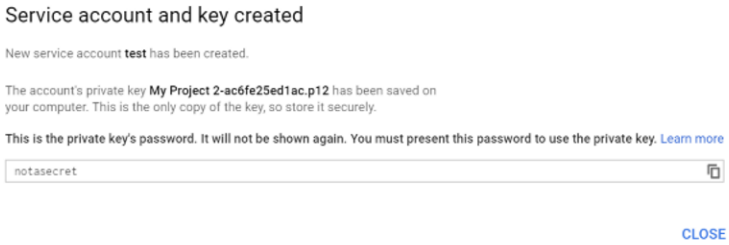
c. From the *Role* list, select *Project* > *Viewer*.

d. Select *P12* as the *Key type* and click *Create*.

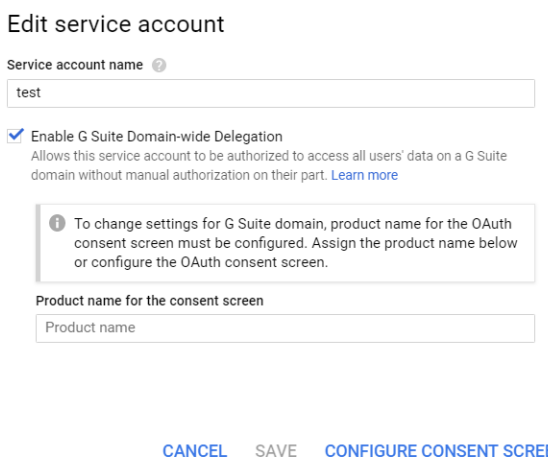


After you create the service account, a private key with the `P12` extension will be saved on your computer.

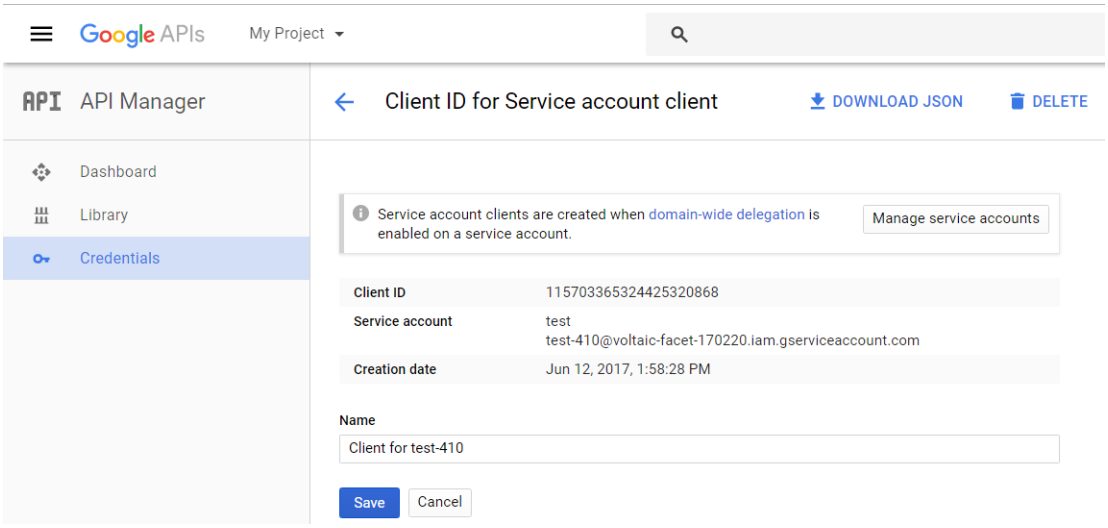
> ⚠ The private key with the `P12` extension is the only copy you will receive. Keep it in a safe place. You should also remember the password prompted on the screen. At this time, that password should be **`notasecret`**.



6. Go to the *Credentials* page > *Manage service accounts*.
7. *Edit* the service account you just created and enable the *Enable Google Apps Domain-Wide Delegation* checkbox. Enter a *Product name for the consent screen* if this field appears.



8. Click *Save*.
9. Click *View Client ID*, and you will see your service account information. Record the client ID, service account, and the associated private key (downloaded in step 5d).



To use the Private Key in EMS, it needs to be converted to `.pem` format. You can use the following `openssl` command to convert it. Remember to use the notasecret password.

```
C:\OpenSSL-Win64\bin>openssl pkcs12 -in demo-
    976b9d6e9328.p12 -out serviceAccount-demo.pem -nodes -
    nocerts
Enter Import Password:
```

Adding Service Account Credentials to Google Admin Console

This section describes how to add the Client ID from the Service Account Credentials to Google Admin console. These settings allow Google to trust FortiClient EMS for Chromebooks, which enables FortiClient EMS for Chromebooks to retrieve information from the Google domain.

To add the client ID:

1. In Google Admin console, go to *Security* > *Advanced settings* > *(you might need to click "show more" to see this)* > *Manage API client access*.
2. Set the following options:
   a. For the *Client Name* option, add the client ID from the Server Account Credentials.
   b. For the *API Scopes* option, add the following string:
   https://www.googleapis.com/auth/admin.directory.orgunit.readonly,https://www.googleapis.com/auth/admin.directory.user.readonly

The API Scopes are case-sensitive and must be lowercase. You might need to copy the string into a text editor and remove spaces created by words wrapping to the second line in the PDF.

3. Click *Authorize*.

Adding Service Account Credentials to EMS

The section describes how to add the Service Account ID and the Service Account Certificate from the Service Account Credentials to FortiClient EMS for Chromebooks.

To add Service Account Credentials:

1. In FortiClient EMS for Chromebooks, go to *View* > *Settings*.
2. Click *EMS for Chromebook*, and set the following options:

The default Service Account Credentials are displayed. Overwrite the default settings with the unique set of Service Account Credentials that you received from Fortinet.

Service Account ID	Displays the configured email address provided for the Service Account Credentials.
New Service Account ID	Type a new email address for the Service Account Credentials.
New Service Account Private Key	Click *Browse*, and select the certificate provided with the Service Account Credentials.

3. Click *Save*.
4. Update the Client ID in the Google Admin Console.

The Service Account Credentials are a set. If you change one of the credentials, you must also change the other two credentials.

FortiClient EMS for Chromebooks Setup

This section describes how to set up FortiClient EMS for Chromebooks. Following is a summary of how to set up FortiClient EMS for Chromebooks:

1. Add an SSL certificate. See Adding SSL certificates on page 26.
2. Add the Google domain. See Adding Google domains on page 28.
3. Create an endpoint profile. See Adding new profiles on page 29.
4. Assign the endpoint profile to the Google domain. See Assigning profiles to Google Chromebooks on page 30.
5. View the status. See Viewing domains on page 31.

Additional configuration procedures are also included in this section.

Adding SSL certificates

This section includes information about the required SSL certificates to support the following types of communication:

- Communication with FortiClient Chromebook Web Filter extension on page 26
- Communication with FortiAnalyzer for logging on page 27

It includes the following procedures:

- Required: Adding SSL certificates to FortiClient EMS for Chromebooks on page 26
- Required only when sending logs to FortiAnalyzer: Adding SSL certificates to FortiAnalyzer on page 28

Communication with FortiClient Chromebook Web Filter extension

The FortiClient Chromebook Web Filter extension communicates with FortiClient EMS for Chromebooks by using HTTPS connections. The HTTPS connections require an SSL certificate. You must obtain an SSL certificate and add the certificate to FortiClient EMS for Chromebooks to allow the extension to trust FortiClient EMS for Chromebooks.

If you use a public SSL certificate, you only need to add the public SSL certificate to FortiClient EMS for Chromebooks. See Adding SSL certificates to FortiClient EMS for Chromebooks on page 26.

However, if you prefer to use a certificate that is not from a common CA, you must add the SSL certificate to FortiClient EMS for Chromebooks, and you must also push the root CA of your certificate to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiClient EMS for Chromebooks will not work. See Uploading root certificates to Google Admin console on page 15.

Adding SSL certificates to FortiClient EMS for Chromebooks

You must add an SSL certificate to FortiClient EMS for Chromebooks to allow HTTPS connections with Google Admin console.

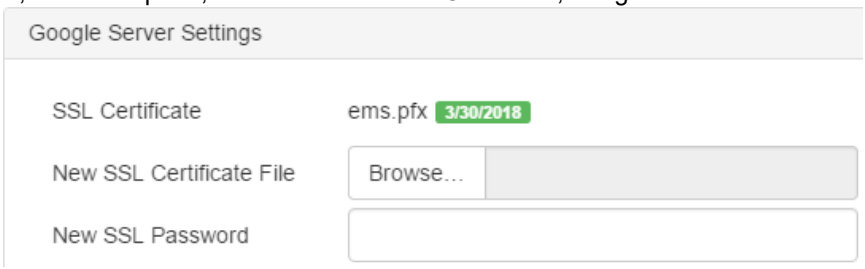
If you are using a public SSL certificate, add the certificate to FortiClient EMS for Chromebooks. You do not need to add the certificate to Google Admin console.

If you are not using a public SSL certificate, you must add the SSL certificate to FortiClient EMS for Chromebooks, and you must add the root certificate to Google Admin console. See Adding root certificates on page 14.

To add or replace SSL certificates:

1. In FortiClient EMS for Chromebooks, go to *View >Settings*.
2. Click the *EMS for Chromebook* tab.
3. Beside *New SSL Certificate File*, click *Browse*, and locate the certificate file (<name>.pfx).
4. In the *New SSL Password* box, type the password.
5. Click *Test*.
6. Click *Save*.

If the SSL certificate is expiring in less than three months, the expiry date label will be yellow; if it has expired, the label will be red. Otherwise, it is green.



Communication with FortiAnalyzer for logging

This section applies only if you are sending logs from FortiClient EMS for Chromebooks to FortiAnalyzer. If you are not sending logs, you can skip this FortiAnalyzer section.

Sending logs to FortiAnalyzer requires that you enable ADOMs in FortiAnalyzer and add FortiClient EMS for Chromebooks to FortiAnalyzer. FortiClient EMS for Chromebooks is added as a device to the FortiClient ADOM in FortiAnalyzer. For information on enabling ADOMs and adding a device to FortiAnalyzer, see the *FortiAnalyzer Administration Guide*.

FortiClient EMS for Chromebooks supports logging to FortiAnalyzer. If you have a FortiAnalyzer device and configure FortiClient EMS for Chromebooks to send logs to FortiAnalyzer, a FortiAnalyzer CLI command must be enabled and an SSL certificate is required to support communication between FortiClient Web Filter extension and FortiAnalyzer.

If you use a public SSL certificate, you only need to add the public SSL certificate to FortiAnalyzer. See Adding SSL certificates to FortiAnalyzer on page 28.

However, if you prefer to use a certificate that is not from a common CA, you must add the SSL certificate to FortiAnalyzer, and you must also push the root CA of your certificate to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiAnalyzer will not work. See Uploading root certificates to Google Admin console on page 15.

The FortiAnalyzer IP address should be specified in the SSL certificate. If you're using a public SSL certificate, the FortiAnalyzer IP address can be assigned to either *Common Name* or *Alternative Name*. If you're using a self-signed (nonpublic) SSL certificate, the *Subject Alternative Name* of your certificate must include `IP:<FortiAnalyzer IP>`.

Enabling HTTP and HTTPS logging access to FortiAnalyzer

You must use the FortiAnalyzer CLI to add HTTP-logging add HTTPS-logging to the allow-access list in FortiAnalyzer. This command is one step in the process that allows FortiAnalyzer to receive logs from FortiClient EMS for Chromebooks.

In FortiAnalyzer CLI, enter the following command:

```
config system interface
   edit "port1"
      set allowaccess https ssh http http-logging https-logging
   next
end
```

Adding SSL certificates to FortiAnalyzer

To add SSL certificates to FortiAnalyzer:

1. In FortiAnalyzer, go to *System Settings* > *Certificates* > *Local Certificates*.
2. Click *Import*. The *Import Local Certificate* dialog box appears.
3. In the *Type* list, select *Certificate*. Or,
   In the *Type* list, select *PKCS #12 Certificate* to upload the certificate in PK12 format.
4. Beside *Certificate File*, click *Browse* to select the certificate.
5. Enter the password and certificate name.
6. Click *OK*.

Selecting certificates for HTTPS connections

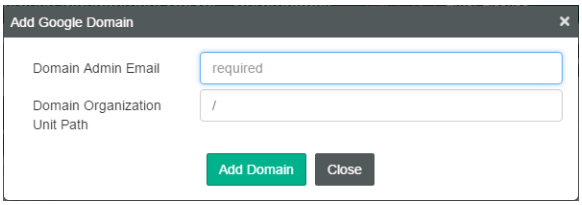
To select certificates for HTTPS connections:

1. In FortiAnalyzer, go to System *Settings* > *Admin* > *Admin Settings*.
2. In the *HTTPS & Web Service Certificate* box, select the certificate you want to use for HTTPS connections, and click *Apply*.

Adding Google domains

To add Google domains:

1. Go to *Google Domains*, and click the *Add a new Google domain* icon (the + button). The *Add Google Domain* dialog box is displayed.



2. In the *Domain Admin Email* box, type your Google domain admin email.
3. In the *Domain Organization Unit Path* box, type the domain organization unit path.

> / stands for the root of the domain.

4. Click *Add Domain*.
   The Google domain information and users are imported into FortiClient EMS for Chromebooks.

Configuring profiles

The profile currently supports web filtering by categories, black and white list, and safe search. You can create different profiles and assign the profiles to different groups in the Google domain.

Adding new profiles

When you install FortiClient EMS for Chromebooks, a default profile is created. This profile is applied to any domains that you add to FortiClient EMS for Chromebooks.

> It is recommended to add Yandex search engine to the black list in the profile.

To create new profiles:

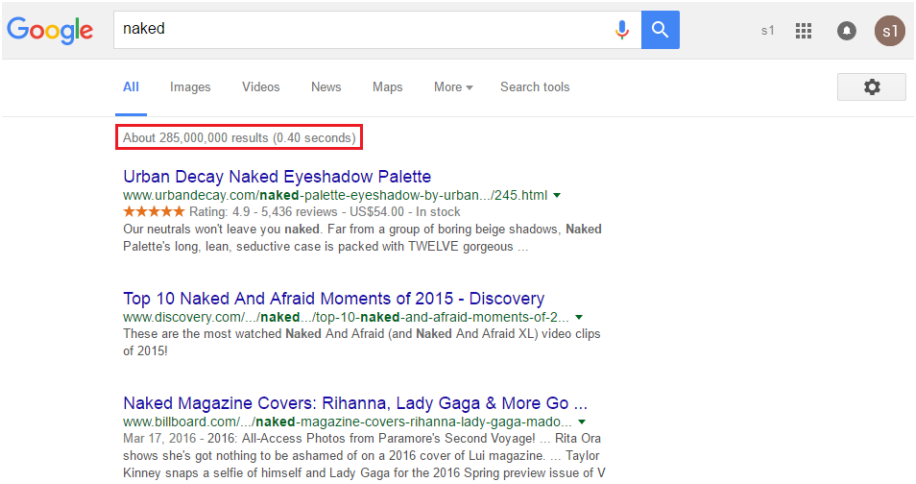
1. Go to *Endpoint Profiles* > *EMS Profiles*, and click *Add a new profile* button (the + button). The *Creating New Profile* pane is displayed.
2. In the *Profile Name* box, type a name for the profile.
3. On the *Web Filter* tab, enable *Web Filter*, and set the web filtering options.
4. On the *System Settings* tab, set the logging options.
5. Click *Save Profile* to save the profile.

Enabling/disabling Safe Search

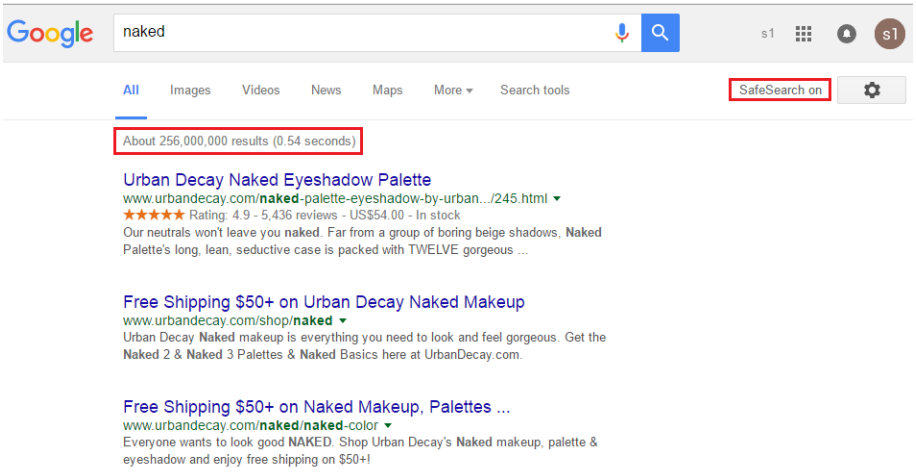
The search engine provides a Safe Search feature that blocks inappropriate or explicit images from search results. The Safe Search feature helps avoid most adult content. FortiClient EMS for Chromebooks supports Safe Search for most common search engines, such as Google, Yahoo, and Bing.

The profile in FortiClient EMS for Chromebooks controls the Safe Search feature.

Following are examples of search results with the Safe Search feature disabled and enabled. Notice the difference between the number of results. Here are the search results when the Safe Search feature is disabled, which has about 285,000,000 results:



Here are the search results when the Safe Search feature is enabled, which has about 256,000,000 results.



To enable or disable Safe Search:

1. In FortiClient EMS for Chromebooks, in the *Endpoint Profiles* area, click the *Default* profile or another profile.
2. On the *Web Filter* tab, enable or disable the *Enable Safe Search* option.

Assigning profiles to Google Chromebooks

After creating the profile, you can assign the profile to Google Domains. When you assign the profile to domains, the profile settings are automatically pushed to the Chromebooks in the domain.

To assign profiles:

1. Go to *Google Domains*
2. Right-click a domain, select *Assign Profile*, and then the profile. The profile is assigned.
3. Hover the mouse over the name of the domain to view the name of the assigned profile.

Viewing domains

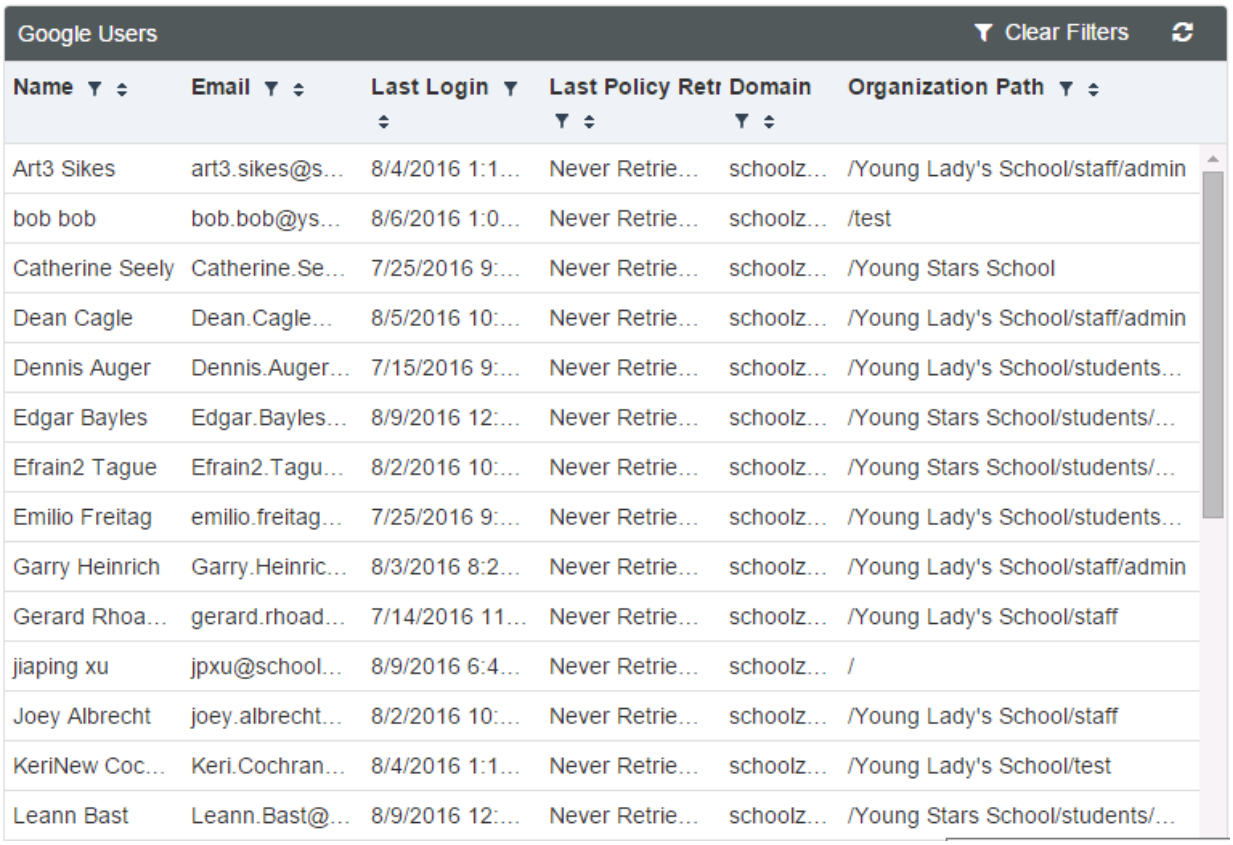
After you add domains to FortiClient EMS for Chromebooks, you can view the list of domains in *Google Domains*. You can also view the list of Google users in each domain as well as details about each Google user in the *User Details*, *Client Statistics*, and *Blocked Sites* panes.

Viewing the Google Users pane

You can view Google Users information in FortiClient EMS for Chromebooks.

To view the Google Users pane:

1. Go to *Google Domains* > *Domains*, and click a domain. The list of Google Users is displayed.



The following options are available in the toolbar:

Clear Filter (filter icon)	Click the Clear Current Filter icon to clear the currently used filter.
Refresh	Click the Refresh icon to refresh the page.

The following columns of information are displayed for Google users:

Name	Name of the Chromebook user.
Email	Email address of the Chromebook user.
Last Login	The date and time for when the user last logged into the domain.
Last Policy Retrieval	The date and time of the last endpoint profile retrieved by Google Chromebook.
Domain	The name of the domain to which the user belongs.
Organizational Path	The organization path in the domain.

Viewing user details

You can view details about each user in a Google domain.

To view user details:

1. Go to *Google Domains* > *Domains*. The list of domains is displayed.
2. Click a domain. The list of Google users is displayed.
3. Click a Google user, and scroll to the bottom of the content pane. The *User Details*, *Client Statistics*, and *Blocked Sites* panes are displayed.

User Details

Field	Information
Name	The name of the user.
Email	Email for the user.
Last Login	The date and time for when the user last logged into the domain.
Last Policy Retrieval	The date and time of the last endpoint profile retrieved by Google Chromebook.
Organization Path	The organization path of the user in the domain.
Effective Policy	The name of the profile assigned to the user in the domain.

Client Statistics

Charts	Information
Blocked Sites Distribution (past <number> days)	The chart displays the distribution of blocked sites in the past number of days. You can configure the number of days for which to display information. Go to *View* > *Settings* > *Log Settings*.
Top 10 Site Categories by Distribution (Past <number> Days)	The chart displays the distribution of top ten site categories in the past number of days. You can configure the number of days for which to display information. Go to *View* > *Settings* > *Log Settings*.

Blocked Sites (Past <number> Days)

Fields	Information
Time	The time the blocked site was visited.
Threat	The type of threat detected.
Client Version	The Chromebook User's current version.
OS	The type of OS used by the Chromebook user.
URL	The URL of the blocked site.
Port	The port number currently listening.
User Initiated	User initiated visitation to the blocked site.

FORTINET®

High Performance Network Security